Cisco Secure VPN Client Wild-Card에 PIX 구성, 사전 공유, No Mode-Config

목차

소개

이 컨피그레이션에서는 와일드카드 및 sysopt **connection permit-ipsec** 및 sysopt ipsec pl-**compatible** 명령을 사용하여 VPN 클라이언트를 PIX 방화벽에 연결하는 방법을 보여 줍니다. 이 문서에서는 nat **0 access-list** 명령도 다룹니다.

참고: 암호화 기술은 내보내기 제어의 대상이 됩니다. 암호화 기술의 수출과 관련된 법을 아는 것은 여러분의 책임입니다. 수출 통제와 관련된 질문이 있는 경우 export@cisco.com으로 이메일을 보내십시오.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 이러한 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure VPN Client 1.0이 포함된 Cisco Secure PIX Software 릴리스 5.0.3(도움말 > 정보 메뉴에 2.0.7 표시) 또는 Cisco Secure VPN Client 1.1이 포함된 Cisco Secure PIX Software 릴

리스 6.2.1(도움말 > 정보 메뉴에 2.1.12 표시).
- 인터넷 시스템은 IP 주소 192.68.0.50을 사용하여 내부의 웹 호스트에 액세스합니다.
- VPN 클라이언트는 모든 포트(10.1.1.0/24 및 10.2.2.0/24)를 사용하여 내부의 모든 시스템에 액세스합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 라이브 네트워크에서 작업하는 경우, 명령을 사용하기 전에 명령의 잠재적인 영향을 이해해야 합니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

배경 정보

PIX에서 **access-list** 및 **nat 0** 명령이 함께 작동합니다. nat **0 access-list** 명령은 sysopt ipsec pl-compatible 명령 대신 **사용됩니다**. nat **0** 명령을 matching access-**list** 명령과 함께 사용하는 경우 NAT를 우회하기 위해 일치하는 ACL(액세스 제어 목록)을 생성하려면 VPN 연결을 만드는 클라이언트의 IP 주소를 알아야 합니다.

참고: sysopt **ipsec pl-compatible** 명령은 일치하는 **access-list** 명령을 사용하여 NAT(Network Address Translation)를 우회하기 위해 nat 0 명령보다 더 잘 확장됩니다. 이유는 연결을 만드는 클라이언트의 IP 주소를 알 필요가 없기 때문입니다. 이 문서의 컨피그레이션에서는 변경 가능한 명령이 굵게 표시됩니다.

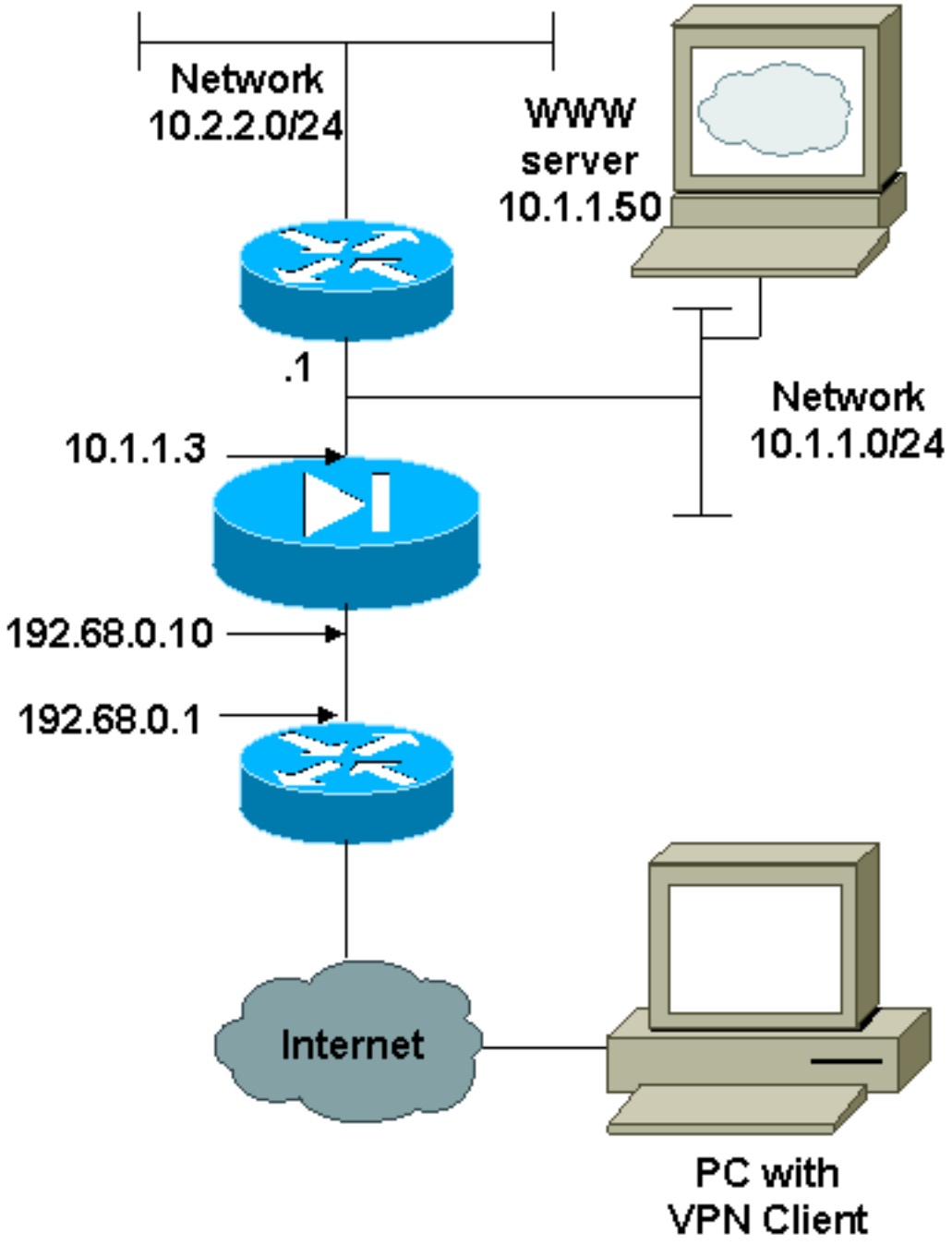
VPN 클라이언트가 있는 사용자는 인터넷 서비스 공급자(ISP)로부터 IP 주소를 연결 및 수신합니다. 사용자는 방화벽 내부의 모든 것에 액세스할 수 있습니다. 여기에는 네트워크가 포함됩니다. 또한 클라이언트를 실행하지 않는 사용자는 정적 할당에서 제공하는 주소를 사용하여 웹 서버에 연결할 수 있습니다. 내부의 사용자는 인터넷에 연결할 수 있습니다. 트래픽이 IPSec 터널을 통과할 필요는 없습니다.

구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

네트워크 다이어그램

이 문서에서는 이 다이어그램에 표시된 네트워크 설정을 사용합니다.



구성

이 문서에서는 여기에 표시된 구성을 사용합니다.

- PIX
- VPN 클라이언트

PIX 컨피그레이션

```
PIX Version 6.2.1
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
```

```
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
!--- The ACL to bypass the NAT. You have to know the !--
- IP address of the Client. In this case, it is !---
subnet 65.10.10.0/24. access-list 103 permit ip 10.0.0.0
255.0.0.0 65.10.10.0 255.255.255.0
pager lines 24
no logging timestamp
no logging standby
logging console debugging
no logging monitor
no logging buffered
no logging trap
logging facility 20
logging queue 512
interface ethernet0 10baset
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 192.68.0.10 255.255.255.0
ip address inside 10.1.1.3 255.255.255.0
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 192.68.0.11-192.168.0.15 netmask
255.255.255.0
!--- Binding ACL 103 to the NAT statement in order to !-
-- avoid NAT on the IPSec packet. nat (inside) 0 access-
list 103
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 192.68.0.50 10.1.1.50 netmask
255.255.255.255 0 0
conduit permit icmp any any
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
route outside 0.0.0.0 0.0.0.0 192.68.0.1 1
route inside 10.2.2.0 255.255.255.0 10.1.1.1 1
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00
udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
!--- The sysopt ipsec pl-compatible command !--- avoids
conduit on the IPSec encrypted traffic. !--- This
command needs to be used if you do not use !--- the nat
0 access-list command.

sysopt ipsec pl-compatible
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map cisco 1 set transform-set myset
crypto map dyn-map 20 ipsec-isakmp dynamic cisco
```

```
crypto map dyn-map interface outside
isakmp enable outside
isakmp key cisco123 address 0.0.0.0 netmask 0.0.0.0
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 1000
telnet timeout 5
terminal width 80
Cryptochecksum:c687aa0afb1dd03abce04c31566b5c52
: end
[OK]
```

VPN 클라이언트 컨피그레이션

```
Network Security policy:
 1- TACconn
     My Identity
          Connection security: Secure
          Remote Party Identity and addressing
          ID Type: IP subnet
          10.0.0.0
           255.0.0.0
          Port all Protocol all

     Connect using secure tunnel
          ID Type: IP address
          192.68.0.10

     Authentication (Phase 1)
     Proposal 1
         Authentication method: pre-shared key
         Encryp Alg: DES
         Hash Alg: MD5
         SA life: Unspecified
         Key Group: DH 1


     Key exchange (Phase 2)
     Proposal 1
         Encapsulation ESP
         Encrypt Alg: DES
         Hash Alg: MD5
         Encap: tunnel
         SA life: Unspecified
         no AH


 2- Other Connections
        Connection security: Non-secure
        Local Network Interface
          Name: Any
          IP Addr: Any
          Port: All
```

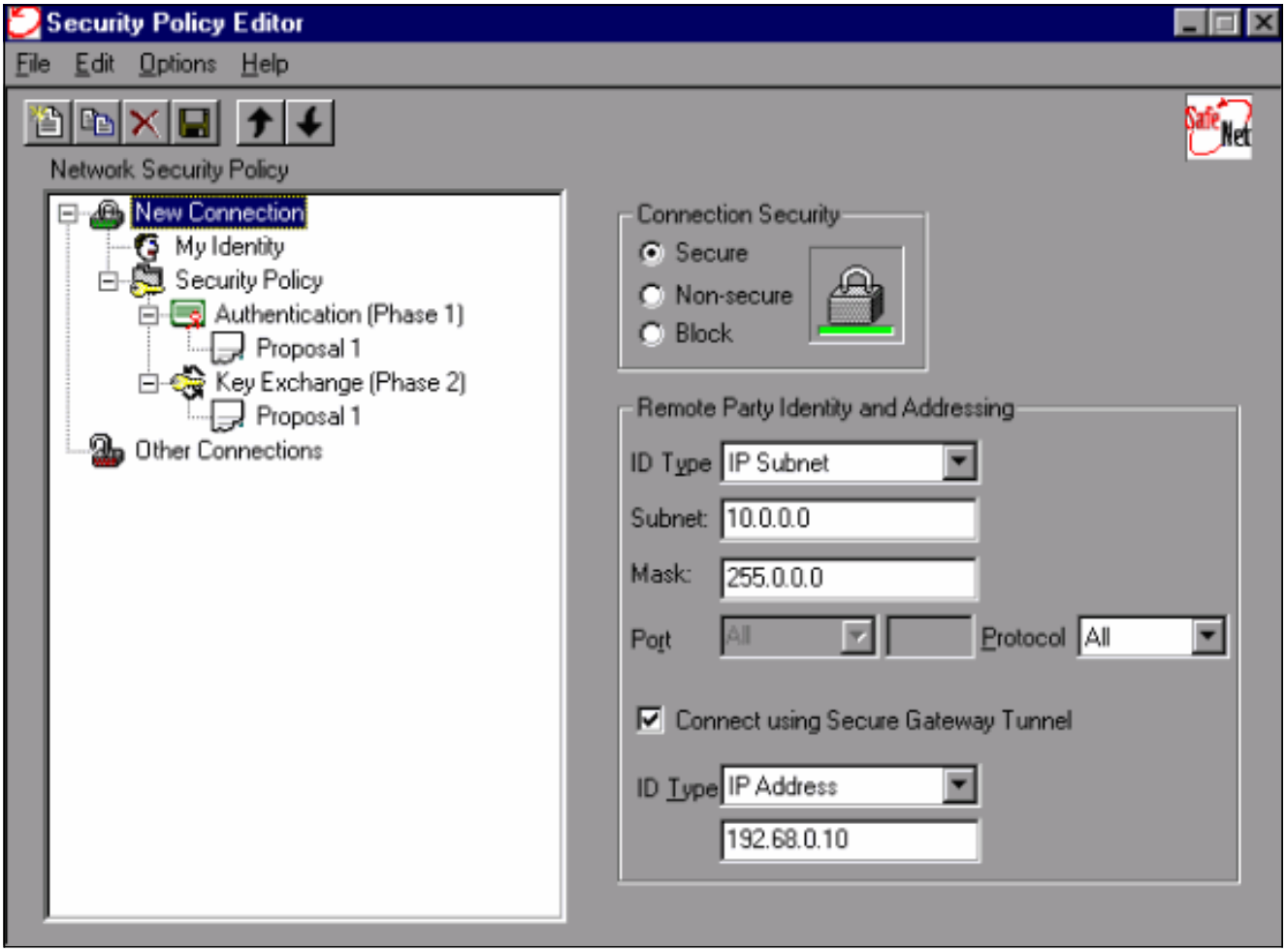
VPN 클라이언트 IPSec 연결에 대한 정책 구성

VPN 클라이언트 IPSec 연결에 대한 정책을 구성하려면 다음 단계를 수행합니다.

1. Remote Party Identity and Addressing(원격 파티 ID 및 주소 지정) 탭에서 VPN 클라이언트를

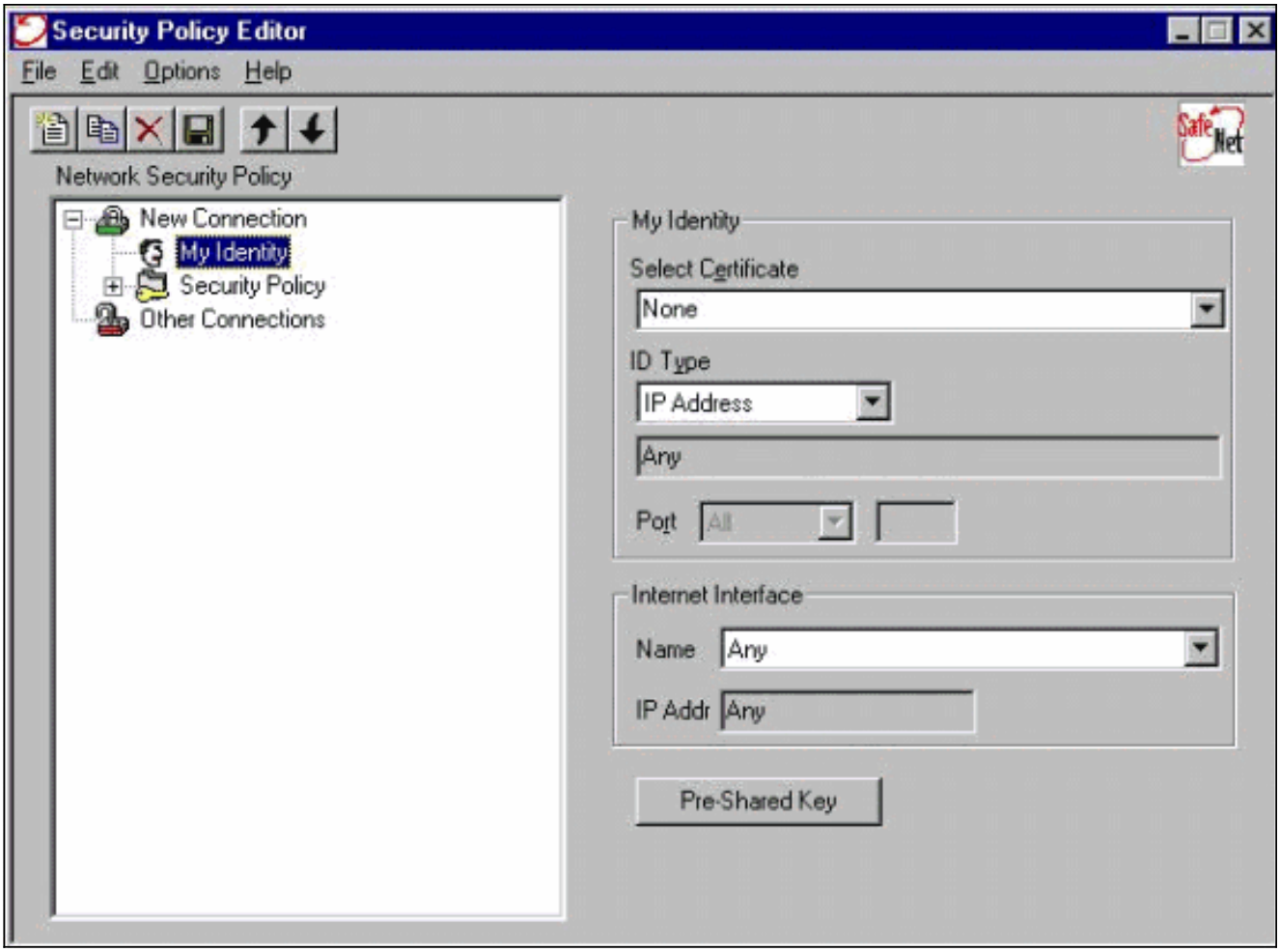
사용하여 연결할 수 있는 사설 네트워크를 정의합니다. 다음으로, **Connect using Secure Gateway Tunnel(보안 게이트웨이 터널을 사용하여 연결)**을 선택하고 PIX의 외부 IP 주소를 정의합니다

.

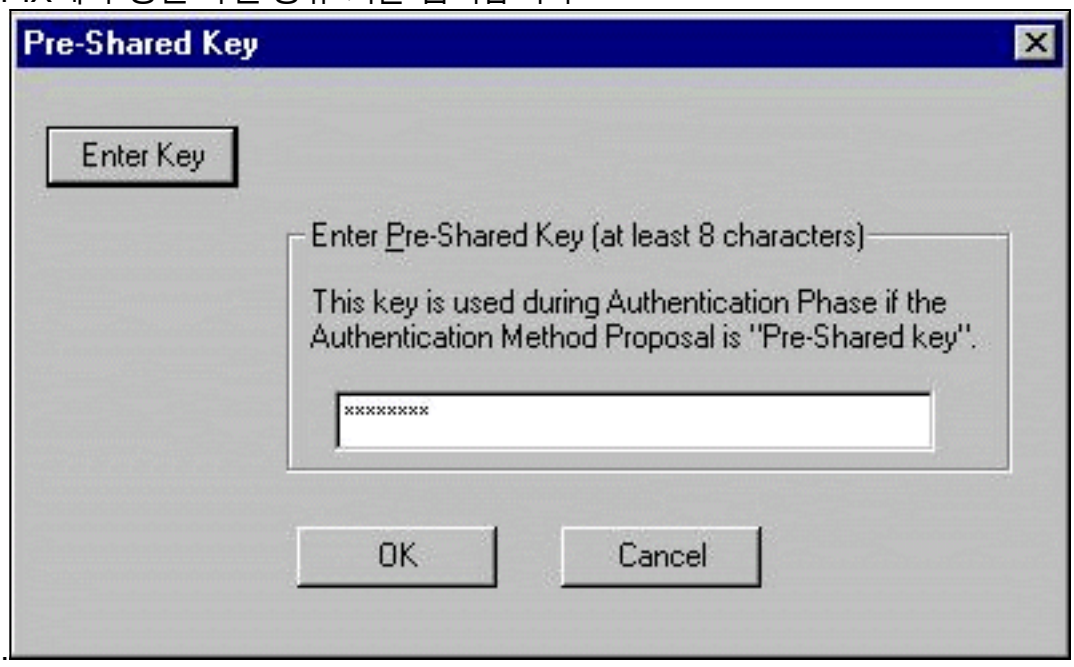


2. **내 ID**를 선택하고 설정을 기본값으로 둡니다. 그런 다음 **사전 공유 키** 버튼을 클릭합니다

.



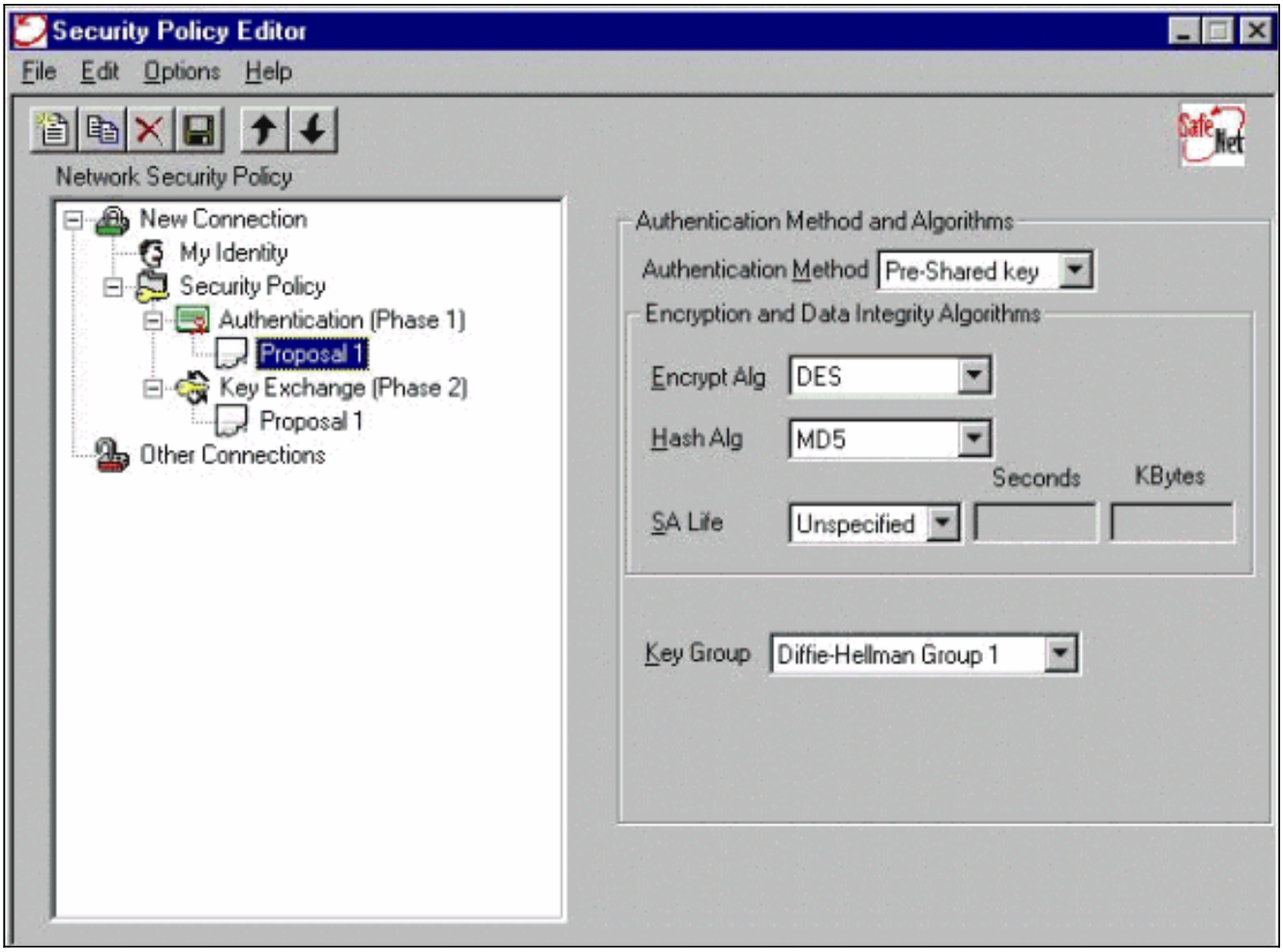
3. PIX에 구성된 사전 공유 키를 입력합니다



.

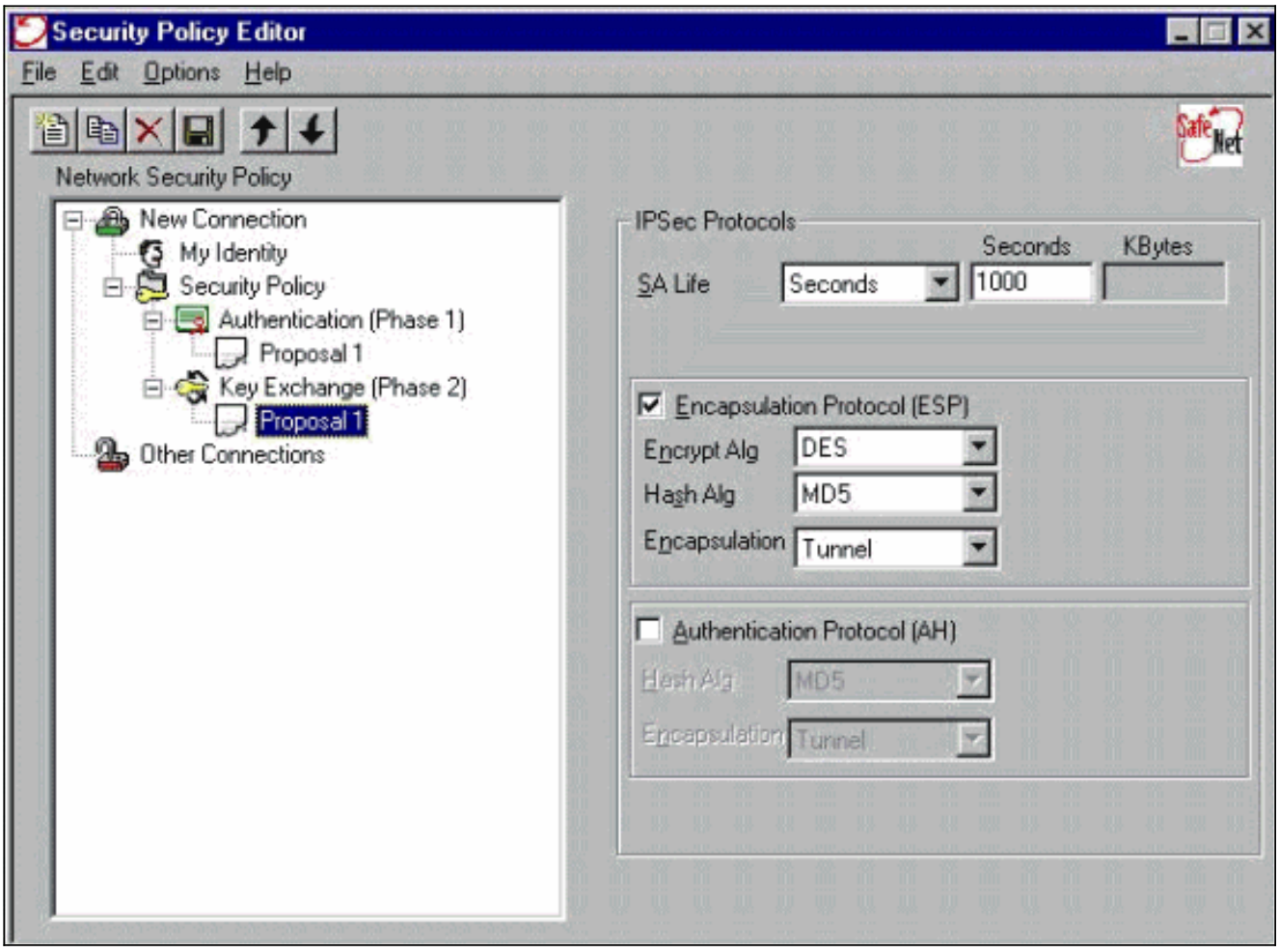
4. 인증 제안(1단계 정책)을 구성합니다

.



5. IPSec 제안(2단계 정책)을 구성합니다

.



참고: 완료되면 정책을 저장하는 것을 잊지 마십시오. 클라이언트에서 터널을 시작하려면 DOS 창을 열고 PIX의 내부 네트워크에서 알려진 호스트를 ping합니다. 터널의 협상을 시도할 때 첫 번째 ping에서 ICMP(Internet Control Message Protocol) 연결 불가 메시지를 수신합니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

debug 명령

참고: debug 명령을 실행하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

클라이언트측 디버그를 보려면 Cisco Secure Log Viewer를 활성화합니다.

- **debug crypto ipsec sa** - 2단계의 IPSec 협상을 표시합니다.
- **debug crypto isakmp sa** - 1단계의 ISAKMP 협상을 표시합니다.
- **debug crypto engine** - 암호화된 세션을 표시합니다.

관련 정보

- Cisco Secure PIX Firewall 명령 참조
- 보안 제품 필드 알림(PIX 포함)
- Cisco PIX 방화벽 소프트웨어 제품 지원
- RFC(Request for Comments)
- IP Security(IPSec) 제품 지원 페이지
- IPSec 네트워크 보안 구성
- 인터넷 키 교환 보안 프로토콜 구성
- IPSec(IP Security) 암호화 소개
- PIX 방화벽을 통한 연결
- IPSec 구성
- 기술 지원 및 문서 – Cisco Systems